National Infrastructure Protection Center
CyberNotes

Issue #2001-01 *January 15, 2001*

CyberNotes is published every two weeks by the National Infrastructure Protection Center (NIPC). Its mission is to support security and information system professionals with timely information on cyber vulnerabilities, malicious scripts, information security trends, virus information, and other critical infrastructure-related best practices.

You are encouraged to share this publication with colleagues in the information and infrastructure protection field. Electronic copies are available on the NIPC Web site at http://www.nipc.gov.

Please direct any inquiries regarding this publication to the Editor-CyberNotes, National Infrastructure Protection Center, FBI Building, Room 11719, 935 Pennsylvania Avenue, NW, Washington, DC, 20535.

Bugs, Holes & Patches

The following table provides a summary of software vulnerabilities identified between December 12, 2000 and January 11, 2001. The table provides the vendor/operating system, software name, potential vulnerability/impact, identified patches/workarounds/alerts, common name of the vulnerability, potential risk, and an indication of whether attacks have utilized this vulnerability or an exploit script is known to exist. Software versions are identified if known. **This information is presented only as a summary; complete details are available from the source of the patch/workaround/alert, indicated in the footnote or linked site.** Please note that even if the method of attack has not been utilized or an exploit script is not currently widely available on the Internet, a potential vulnerability has been identified. **Updates to items appearing in previous issues of CyberNotes are listed in bold. New information contained in the update will appear as red and/or italic text.** Where applicable, the table lists a "CVE number" (in red) which corresponds to the Common Vulnerabilities and Exposures (CVE) list, a compilation of standardized names for vulnerabilities and other information security exposures.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Alt-N Technologies[1]	Windows 95/98/NT 4.0/2000	MDaemon 3.5.0	A Denial of Service vulnerability exists due to the way buffers are handled within the IMAP and webconfig services.	Upgrade available at: http://mdaemon.deerfield.com/download/getmdaemon.cfm	MDaemon Denial of Service	Low	Bug discussed in newsgroups and websites.

[1] Defcom Labs Advisory, def-2000-03, December 19, 2000.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
America OnLine, Inc.[2]	Windows 95/98/ CE 2.0/3.0/NT 4.0/2000, MacOS 9.0	AOL Instant Messenger (AIM) 3.5.1856, 4.0, 4.1.2010, 4.2.1193	Multiple buffer overflow vulnerabilities exist which could give a remote malicious user the ability to alter program execution. **Note:** You do not need to be running AIM, but merely have it installed to be vulnerable.	This vulnerability has been addressed in AOL Instant Messenger 4.3.2229 available at: http://www.aol.com/aim/download.html	AOL Instant Messenger Multiple Vulnerabilities CVE name: CAN-2000-1093, CAN-2000-1094	**High**	Bug discussed in newsgroups and websites. Exploit has been published. Vulnerability has appeared in the Press and other public media.
Apple[3]	MacOS 7.0-9.0	Macintosh Runtime for Java 2.2.3	A vulnerability exists in MRJ (Mac OS Runtime for Java) due to a failure to enforce security controls when the values of the ARCHIVE parameter and the CODEBASE parameter conflict. This could allow a malicious Java applet downloaded from a website to access the local filesystem or unauthorized websites when executed.	No workaround or patch available at time of publishing.	Macintosh MRJ Unauthorized File Access	Medium	Bug discussed in newsgroups and websites.
BEA Systems [4]	Windows 98/NT 4.0, Unix	Weblogic Server 4.5x, 5.1x	An unchecked buffer overflow vulnerability exists which could let a malicious user crash the system or execute arbitrary code.	Upgrade available at: http://commerce.beasys.com/downloads/weblogic_server.jsp	WebLogic Server Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
Borland/ Inprise[5]	Windows NT 4.0/2000, Unix	Interbase 4.0, 5.0, 6.0; Open source Interbase 6.0, 6.01; Open source Firebird 0.9.3 and previous	A vulnerability exists because a backdoor account with a known password exists which could let a malicious user login to services on TCP port 3050 and access the database. If the database software is running with root privileges, then any file on the server's file system can be overwritten, possibly leading to execution of arbitrary commands as root.	Patch available at: http://inprise-svca.www.conxion.com/	Interbase Backdoor Password CVE name: CAN-2001-0008	**High**	Bug discussed in newsgroups and websites. Exploit has been published. Vulnerability has appeared in the Press and other public media.
Brian Stanback[6]	Multiple	bsguest.cgi 1.0	Vulnerabilities exist in the bsguest (a guestbook script)) and bslist (a mailing list script) which could let a malicious user run arbitrary shell commands.	Vulnerabilities have been patched in the latest release.	Brian Stanback Multiple CGI Vulnerabilities	**High**	Bug discussed in newsgroups and websites. Exploits have been published.

[2] @stake Inc. Security Advisory, A121200-1, December 12, 2000.

[3] Bugtraq, December 15, 2000.

[4] Defcom Labs Advisory, def-2000-04, December 19, 2000.

[5] CERT® Advisory CA-2001-01, January 11, 2001.

[6] Bugtraq, December 21, 2000.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Check Point Software[7]	Multiple	Firewall-1 4.1 SP2	A vulnerability exists in the "Fast Mode" option which may allow a malicious user to bypass access control restrictions and access certain blocked services normally protected by the firewall ruleset.	Upgrade available at: http://www.checkpoint.com/cgi-bin/download.cgi	Firewall-1 Fast Mode TCP Fragment	Medium/ **High** **(High if DDoS best-practices not in place)**	Bug discussed in newsgroups and websites. Exploit script has been published.
Debian[8]	Unix	Linux 2.2, 2.2 68k, alpha, arm, powerpc, sparc	A vulnerability exists in the way dialog creates lock-files, which could allow a malicious user to truncate, corrupt, or overwrite sensitive files.	Upgrade available at: http://security.debian.org/dists/stable/updates/main/	Dialog /tmp File Race Condition	Medium	Bug discussed in newsgroups and websites.
Extropia[9]	Unix	bbs_forum.cgi 1.0	A vulnerability exists in the way the program handles the 'read' parameter that could let a remote malicious user execute arbitrary code.	Patch available at: http://www.extropia.com/hacks/bbs_security.html	Bbs_forum.cgi Remote Arbitrary Command Execution	**High**	Bug discussed in newsgroups and websites.
FreeBSD[10]	Unix	FreeBSD 3.x, 4.1, 4.1.1, 4.2	Several security vulnerabilities exist in the procfs code that could let a malicious user cause anything from a Denial of Service to a local root compromise.	Patch available at: ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches	FreeBSD Procfs Vulnerabilities	Low/**High**	Bug discussed in newsgroups and websites. Exploit has been published.
Hewlett-Packard[11]	Unix	HP-UX 10.1, 10.10, 10.20, 11.0	A buffer overflow vulnerability exists in the kermit software package distributed with HP-UX, which could allow a malicious user to arbitrarily execute code, and gain elevated privileges with the potential for administrative access.	Upgrades available at: http://itrc.hp.com	HP-UX Kermit Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
Hewlett-Packard[12]	Unix	UP-UX 10.xx, 11.0	A vulnerability exists in the program /usr/bin/top, which could let a malicious user modify files writable by group "sys."	Upgrades available at: http://itrc.hp.com	HP-UX Top Modify Files	Medium	Bug discussed in newsgroups and websites.
Hewlett-Packard[13]	Unix	HP-UX 10.20, 11.0	A vulnerability exists in the creation of files by the stm (Support Tools Manager) in the directory /var/log/stm that could let a malicious user gain elevated privileges.	A temporary fix to this problem is to change the permissions on /var/stm/log to 0600.	HP-UX Stm Race Condition	Medium	Bug discussed in newsgroups and websites.

[7] Bugtraq, December 18, 2000.

[8] Debian Security Advisory, DSA-008-1, December 25, 2000.

[9] Cgisecurity.com Advisory #3.1, January 7, 2001.

[10] FreeBSD Security Advisory, FreeBSD-SA-00:77, reissued December 29, 2000.

[11] Hewlett-Packard Company Security Bulletin, HPSBUX0012-135, December 21, 2000.

[12] Hewlett-Packard Company Security Bulletin, HPSBUX0012-134, December 18, 2000.

[13] Securiteam, January 9, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
IBM[14]	Windows NT 4.0, Unix	HTTP Server 1.3.12.2	A Denial of Service vulnerability exists in ApfaCache when certain types of URLs are requested.	**Workaround:** "This issue is caused by a problem in the AfpaCache module of the IBM HTTP Server. The only workaround at this time is to disable the AfpaCache. IBM Development is working on fixing this issue, but it is not yet known when a fix will be available."	HTTP Server AfpaCache Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit has been published.
IBM[15]	Windows NT 4.0/2000, OS/2, OS/390 Unix	Lotus Domino 5.0.2, 5.0.3, 5.0.5, 5.0.6	A directory traversal vulnerability exists which could allow a remote malicious user to gain access to systems files, password files, etc. This could lead to a complete compromise of the host.	No workaround or patch available at time of publishing.	Lotus Domino Server Directory Traversal	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
ibrow[16]	Multiple	newsdesk.cgi 1.2	A directory traversal vulnerability exists which could allow a malicious user to obtain passwords and other sensitive information.	No workaround or patch available at time of publishing.	Newsdesk.cgi File Disclosure	Medium	Bug discussed in newsgroups and websites.
Infinite[17]	Windows 95/98/NT 4.0/2000	Interchange 3.61	A Denial of Service vulnerability exists when a malformed POST command to the HTTP is requested, which could let a malicious user possibly execute arbitrary code.	No workaround or patch available at time of publishing.	InterChange Denial of Service	Low/**High**	Bug discussed in newsgroups and websites. Exploit has been published.
Informix[18]	Multiple	Webdriver 1.0	A vulnerability exists due to insecure methods of temporary file creation, which could let a malicious user execute arbitrary files.	No workaround or patch available at time of publishing.	Webdriver Local File Overwrite	**High**	Bug discussed in newsgroups and websites.
Informix[19]	Multiple	Webdriver 1.0	A vulnerability exists if the webdriver is called directly without any additional parameters included in the URL, which could let a remote malicious user access the system's administration functions.	No workaround or patch available at time of publishing.	Webdriver Remote Administration Access	**High**	Bug discussed in newsgroups and websites. Exploit has been published.

[14] Defcom Labs Advisory, def-2001-02, January 8, 2001.
[15] Georgi Guninski Security Advisory #32, January 5, 2001.
[16] Bugtraq, January 4, 2001.
[17] Strumpf Noir Society Advisories, December 21, 2000.
[18] Bugtraq, January 4, 2001.
[19] Bugtraq, December 30, 2000.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Macromedia, Inc.[20]	Windows 95/98/NT 4.0, MacOS 9.0, Unix	Shockwave Flash 8.0 and Previous	A Denial of Service vulnerability exists in the Flash plugin when it encounters a maliciously or incorrectly created SWF file.	No workaround or patch available at time of publishing.	Shockwave Flash SWF Denial of Service	Low	Bug discussed in newsgroups and websites. Vulnerability has appeared in the Press and other public media.
Michael Glickman[21]	Unix	itetris 1.6.1, 1.6.2	A vulnerability exists in the system() function which may allow a malicious user to execute arbitrary commands as root.	No workaround or patch available at time of publishing.	Itetris Privileged Arbitrary Command Execution	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
Microsoft[22]	Windows 95/98/NT 4.0/2000	Windows ME, 2000, Office 2000	A vulnerability exists in the Web Extender Client (WEC) which could let a malicious user obtain sensitive information and possibly assist in further attacks.	Patch available at: http://www.microsoft.com/technet/security/bulletin/ms01-001.asp	Windows Web Client Extender NTLM Authentication	Medium	Bug discussed in newsgroups and websites.
Microsoft[23]	Windows 95/98/NT 4.0/2000	Windows Media Player 7	A security vulnerability exists that is exploitable through IE, which could allow a malicious user to execute arbitrary commands.	Unofficial workaround (Georgi Guninski): Disable Active Scripting	Windows Media Player Javascript URL	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
Microsoft[24]	Windows 95/98/NT 4.0/2000	Internet Explorer 5.01, 5.5	A Denial of Service vulnerability exists when malformed arguments are sent to the mstask.exe service.	No workaround or patch available at time of publishing.	Internet Explorer 'mstask.exe' CPU Consumption	Low	Bug discussed in newsgroups and websites. Exploit has been published.
Microsoft[25]	Windows NT 2000	Windows NT 2000 Server, Advanced Server	A vulnerability exists in the domain controllers, which could let a malicious user gain administrator privileges.	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/security/bulletin/fq00-099.asp	Windows Directory Service Restore Mode Password	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
Microsoft[26]	Windows NT 4.0	Internet Information Service (IIS) 4.0, 5.0	A vulnerability exists in the FrontPage Server Extensions, which could allow a remote malicious user to cause a Denial of Service.	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/security/bulletin/fq00-100.asp	IIS Malformed Web Form Submission	Low	Bug discussed in newsgroups and websites.

[20] Bugtraq, December 20, 2000.
[21] Bugtraq, December 19, 2000.
[22] Microsoft Security Bulletin, MS01-001, January 11, 2001.
[23] Georgi Guninski Security Advisory #31, January 1, 2001.
[24] eSecurityOnline.com Free Vulnerability Alert 3233, December 14, 2000.
[25] Microsoft Security Bulletin, MS00-099, December 20, 2000.
[26] Microsoft Security Bulletin, MS00-100, December 22, 2000.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft[27]	Windows NT 4.0/2000	Index Server 2.0, Indexing Service 3.0	A vulnerability exists which could allow a malicious web site operator to learn the names and properties of files and folders on the machine of a visiting user.	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/security/bulletin/fq00-098.asp	Indexing Service File Enumeration	Medium	Bug discussed in newsgroups and websites.
Microsoft[28]	Windows NT 4.0/2000	Windows Media Services 4.0, 4.1	A security vulnerability exists which could allow a malicious user to cause a Denial of Service.	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/security/bulletin/fq00-097.asp	Severed Windows Media Server Connection	Low	Bug discussed in newsgroups and websites.
Multiple Vendors[29]	Unix	Max-Wilhelm Bruker bftpd 1.0.13	A buffer overflow vulnerability exists when the SITE CHOWN command is requested to change the ownership of a file, which could let a remote malicious user gain root access.	Unofficial workaround (Securiteam): Replace in /etc/bftpd.conf: ENABLE_SITE=yes By ENABLE_SITE=no	Max-Wilhelm Bruker Bftpd Buffer Overflow	**High**	Bug discussed in newsgroups and websites.
Multiple Vendors[30]	Unix	GNU Emacs 20.6 and Previous	A vulnerability exists in the permission settings of the slave terminal, which could allow a malicious user on a multi-user system to eavesdrop on, or forge responses to, an Emacs client.	Upgrade available at: http://sunsite.ualberta.ca/pub/Mirror/Linux/mandrake/updates	Emacs Inadequate PTY Permissions	Medium	Bug discussed in newsgroups and websites.
Multiple Vendors[31]	Unix	GTK GTK+ 1.2.8 and Previous	A vulnerability exists in the Gimp Toolkit, which could allow a malicious user to gain elevated privileges, overwrite system files, or execute arbitrary code.	No workaround or patch available at time of publishing.	GTK+ Arbitrary Loadable Module Execution	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
Multiple Vendors[32]	Unix	Stunnel prior to 3.9	Multiple vulnerabilities exist: the PRNG (pseudo-random generated) is not seeded correctly which could lead to weak encryption on machines that lack /dev/random such as Solaris and Windows; Pid files are not created securely, making Stunnel vulnerable to a symlink attack; and an insecure syslog() call exists which could be exploited to gain elevated privileges.	Upgrade available at: http://www.stunnel.org/download/stunnel/src/stunnel-3.9.tar.gz	Multiple Stunnel Vulnerabilities	**High**	Bug discussed in newsgroups and websites. Exploit has been published.

[27] Microsoft Security Bulletin, MS00-098, December 19, 2000.
[28] Microsoft Security Bulletin, MS00-097, December 15, 2000.
[29] Securiteam, January 9, 2001.
[30] Linux-Mandrake Security Update Advisory, MDKSA-2000:088, December 31, 2000.
[31] Bugtraq, January 3, 2001.
[32] Securiteam, December 21, 2000.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Multiple Vendors[33]	Unix	Chris Allegretta Nano 0.7-0.7.9, 0.8.1-0.8.9, 0.9.1, 0.9.10-0.9.19, 0.9.2-0.9.22	A Denial of Service vulnerability exists when a session terminates unexpectedly.	Upgrade available at: http://security.debian.org/dists/stable/updates/main/source/	Nano Local File Overwrite	Low	Bug discussed in newsgroups and websites.
Multiple Vendors[34]	Unix	Judd Montgomery jpilot 0.98.1 and Previous	A vulnerability exists in the jpilot directory, which could allow malicious users to gain unauthorized access to sensitive information.	**Linux-Mandrake:** http://www.linux-mandrake.com/en/ftp.php3	Jpilot Directory Sensitive Information	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
Multiple Vendors[35]	Unix	Digital (Compaq) TRU64/DIGITAL UNIX 5.0; HP HP-UX 9.0; SGI IRIX 6.2, 6.5.5, 6.5.7; Sun Solaris 2.5.1, 2.6, 7.0	A vulnerability exists in redirection using the << operator, which could let a malicious user corrupt files owned by another user, or append content to other sensitive system files.	No workaround or patch available at time of publishing.	Korn Shell Redirection Race Condition	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
Multiple Vendors[36]	Unix	RedHat Linux 7.0; Wirex Immunix OS 7.0-Beta	A race condition vulnerability exists in the creation and handling of /tmp files that could let a malicious user overwrite or append system files.	Upgrade available at: **Wirex Immunix OS 7.0-Beta:** http://www.immunix.org/ImmunixOS/7.0-beta/updates/RPMS/linuxconf-devel-1.19r2-4_StackGuard_2.i386.rpm	Linuxconf /tmp File Race Condition	Medium	Bug discussed in newsgroups and websites.
Multiple Vendors[37]	Unix	Debian Linux 2.3; GNU glibc 2.1.9 and greater; RedHat Linux 7.0; Terra Soft Solutions, Inc. Yellow Dog Linux 2.0	A vulnerability exists which could let a malicious user compromise system accounts, elevated privileges, and potentially gain administrative access.	No workaround or patch available at time of publishing.	Glibc RESOLV_HOST_CONF File Read Access	Medium	Bug discussed in newsgroups and websites. Exploit has been published.

[33] Debian Security Advisory, DSA-004-1, December 16, 2000.
[34] Bugtraq, December 14, 2000.
[35] Bugtraq, December 21, 2000.
[36] Immunix OS Security Advisory, IMNX-2000-70-019-01, January 10, 2001.
[37] Bugtraq, January 10, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Multiple Vendors[38]	Unix	RedHat Linux 7.0; Wirex Immunix OS 7.0-Beta	A race condition vulnerability exists in the creation and handling of /tmp files that could let a malicious user overwrite or append system files.	Upgrade available at: **Wirex Immunix OS 7.0-Beta:** http://www.immunix.org/ImmunixOS/7.0-beta/updates/RPMS	Apache /tmp File Race	**High**	Bug discussed in newsgroups and websites.
Multiple Vendors[39] ***More upgrades available[40]***	**Unix**	**Colten Edwards BitchX 1.0c17** ***FreeBSD 3.5.1, 4.2 ; Conectiva Linux 4.0, 4.0es, 4.1, 4.2, 5.0, prg gráficos, ecommerce, 5.1, 6.0; Linux-Mandrake 6.1, 7.0, 7.1, 7.2***	**Two security vulnerabilities exist which could allow a remote malicious user to execute arbitrary code.**	**Upgrade to the latest package available:** **RedHat:** **ftp://updates.redhat.com/powertools/** **OpenLinux:** **ftp://ftp.calderasystems.com/pub/updates/** ***Conectiva-Linux:*** ***ftp://atualizacoes.conectiva.com.br/*** ***FreeBSD:*** ***ftp.FreeBSD.org/pub/FreeBSD/ports/i386/packages-3-stable/irc/BitchX-1.0c17_1.tgz*** ***Linux-Mandrake:*** ***http://www.linux-mandrake.com/en/ftp.php3***	**BitchX Multiple Vulnerabilities**	**High**	**Bug discussed in newsgroups and websites. Exploit script has been published.**
Multiple Vendors[41]	Windows NT 4.0/2000, Unix	ikonboard 2.1.7b and previous	A vulnerability exists in the operation of the register.cgi script which could allow a remote malicious user to gain access to restricted resources execute arbitrary commands.	Contact your vendor for patch.	Ikonboard Arbitrary Command Execution	**High**	Bug discussed in newsgroups and websites.
Multiple Vendors[42] [43]	Unix	Mandrake Soft Linux 6.0, 6.1, 7.0, 7.1, 7.2; RedHat Linux 7.0; Wirex Immunix OS 7.0-Beta	A temporary file race vulnerability exists in the useradd program contained in the shadow-utils package that could let a malicious user overwrite or append to and corrupt files writable by the UID of the passwd process.	Upgrades available at: **Linux-Mandrake:** http://sunsite.ualberta.ca/pub/Mirror/Linux/mandrake/ **Wirex Immunix:** http://www.immunix.org/ImmunixOS/7.0-beta/updates/RPMS/shadow-utils-19990827-18_StackGuard_2.i386.rpm	Shadow-utils /etc/default Temp File Race Condition	Medium	Bug discussed in newsgroups and websites.
Multiple Vendors[44] [45]	Unix	Mandrake Soft Linux 6.0, 6.1, 7.0, 7.1, 7.2; RedHat Linux 7.0; Wirex Immunix OS 7.0-Beta	A race condition vulnerability exists in the creation and handling of /tmp files that could let a malicious user overwrite or append system files.	Upgrades available at: **Wirex Immunix:** http://www.immunix.org/ImmunixOS/7.0-beta/updates/RPMS/rdist-6.1.5-14_StackGuard _2.i386.rpm **Linux-Mandrake:** http://sunsite.ualberta.ca/pub/Mirror/Linux/mandrake/	Rdist /tmp File Race Condition	Medium	Bug discussed in newsgroups and websites.

[38] Immunix OS Security Advisory, IMNX-2000-70-016-01, January 10, 2001.
[39] eSecurityOnline.com Free Vulnerability Alert 3227, December 14, 2000.
[40] Securiteam, January 2, 2001.
[41] Bugtraq, December 28, 2000.
[42] Immunix OS Security Advisory, IMNX-2000-70-027-01, January 10, 2001.
[43] Linux-Mandrake Security Update Advisory, MDKSA-2001:007, January 10, 2001.
[44] Immunix OS Security Advisory, IMNX-2000-70-026-01, January 10, 2001.
[45] Linux-Mandrake Security Update Advisory, MDKSA-2001:005, January 10, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Multiple Vendors[46] [47]	Unix	Soft Linux 6.0, 6.1, 7.0, 7.1, 7.2; RedHat Linux 7.0; Wirex Immunix OS 7.0-Beta	A race condition vulnerability exists in the creation and handling of /tmp files that could let a malicious user overwrite or append system files.	Upgrades available at: **Wirex Immunix:** http://www.immunix.org/ImmunixOS/7.0-beta/updates/RPMS/getty_ps-2.0.7j-12_StackGuard_2.i386.rpm **Linux-Mandrake:** http://sunsite.ualberta.ca/pub/Mirror/Linux/mandrake/	Getty_ps /tmp File Race Condition	Medium	Bug discussed in newsgroups and websites.
Multiple Vendors[48, 49]	Unix	RedHat Linux 7.0; Wirex Immunix OS 7.0-Beta; Linux-Mandrake 6.0, 6.1, 7.0, 7.1, 7.2	A race condition vulnerability exists in the creation and handling of /tmp files that could let a malicious user overwrite or append system files.	Upgrade available at: **Wirex Immunix OS 7.0-Beta:** http://www.immunix.org/ImmunixOS/7.0-beta/updates/RPMS/gpm-1.19.3-4_StackGuard_2.i386.rpm **Linux-Mandrake:** http://www.linux-mandrake.com/en/ftp.php3	Gpm /tmp File Race Condition	Medium	Bug discussed in newsgroups and websites.
Multiple Vendors[50, 51]	Unix	David Madore ftpd-BSD 0.2.3; NetBSD 1.4, 1.4.1, 1.4.2, 1.5; OpenBSD 2.4-2.8	A buffer overflow vulnerability exists in the replydirname() function, which could compromise root access.	**David Madore:** http://www.samiam.org/rpms/ftpd-BSD-0.2.3-4.i386.rpm **NetBSD:** ftp://ftp.NetBSD.ORG/pub/NetBSD/misc/security/patches/20001220-ftpd-1.5 **OpenBSD:** http://www.securityfocus.com/data/vulnerabilities/patches/005_ftpd.patch	BSD Ftpd Single Byte Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Exploit script has been published. Vulnerability has appeared in the Press and other public media.
Multiple Vendors[52, 53]	Unix	RedHat Linux 7.0; Wirex Immunix OS 7.0-Beta; Linux-Mandrake 6.0, 6.1, 7.0, 7.1, 7.2	A race condition vulnerability exists in sdiff program, which could let a malicious user overwrite or append system files.	Upgrade available at: **Wirex Immunix OS 7.0-Beta:** http://www.immunix.org/ImmunixOS/7.0-beta/updates/RPMS/diffutils-2.7-21_StackGuard_2.i386.rpm **Linux-Mandrake:** http://www.linux-mandrake.com/en/ftp.php3	Sdiff /tmp File Race Condition	Medium	Bug discussed in newsgroups and websites.

[46] Immunix OS Security Advisory, IMNX-2000-70-025-01, January 10, 2001.
[47] Linux-Mandrake Security Update Advisory, MDKSA-2001:004, January 10, 2001.
[48] Immunix OS Security Advisory, IMNX-2000-70-021-01, January 10, 2001.
[49] Linux-Mandrake Security Update Advisory, MDKSA-2001:006, January 10, 2001.
[50] OpenBSD Security Advisory, December 18, 2000.
[51] Bugtraq, December 18, 2000.
[52] Immunix OS Security Advisory, IMNX-2000-70-024-01, January 10, 2001.
[53] Linux-Mandrake Security Update Advisory, MDKSA-2001:008, January 10, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Multiple Vendors[54, 55]	Unix	RedHat Linux 7.0; Wirex Immunix OS 7.0-Beta; Linux-Mandrake 6.0, 6.1, 7.0, 7.1, 7.2	A race condition vulnerability exists in the creation and handling of /tmp files that could let a malicious user overwrite or append system files.	Upgrade available at: **Wirex Immunix OS 7.0-Beta:** http://www.immunix.org/ImmunixOS/7.0-beta/updates/RPMS/inews-2.2.3-3_StackGuard_3.i386.rpm **Linux-Mandrake:** http://www.linux-mandrake.com/en/ftp.php3	Inn /tmp File Race Condition	Medium	Bug discussed in newsgroups and websites.
Multiple Vendors[56, 57]	Unix	RedHat Linux 7.0; Wirex Immunix OS 7.0-Beta; Linux-Mandrake 6.0, 6.1, 7.0, 7.1, 7.2	A race condition vulnerability exists in the creation and handling of files in the /tmp directory which could let a malicious user overwrite or append system files.	Upgrade available at: **Wirex Immunix OS 7.0-Beta:** http://www.immunix.org/ImmunixOS/7.0-beta/updates/RPMS/wu-ftpd-2.6.1-6_StackGuard_2.i386.rpm **Linux-Mandrake:** http://www.linux-mandrake.com/en/ftp.php3	Wu-ftpd /tmp File Race Condition	Medium	Bug discussed in newsgroups and websites.
Multiple Vendors[58, 59]	Unix	RedHat Linux 7.0; Wirex Immunix OS 7.0-Beta; Linux-Mandrake 6.0, 6.1, 7.0, 7.1, 7.2	A race condition vulnerability exists in the creation and handling of /tmp files that could let a malicious user overwrite or append system files.	Upgrade available at: **Wirex Immunix OS 7.0-Beta:** http://www.immunix.org/ImmunixOS/7.0-beta/updates/RPMS/ **Linux-Mandrake:** http://www.linux-mandrake.com/en/ftp.php3	Mgetty /tmp File Race Condition	Medium	Bug discussed in newsgroups and websites.
Multiple Vendors[60, 61]	Unix	National Science Foundation Squid Web Proxy 2.3STABLE4; RedHat Linux 7.0; Wirex Immunix OS 7.0-Beta; Linux-Mandrake 6.0, 6.1, 7.0, 7.1, 7.2	A race condition vulnerability exists in the creation and handling of /tmp files that could let a malicious user overwrite or append system files.	Upgrade available at: **Wirex Immunix OS 7.0-Beta:** http://www.immunix.org/ImmunixOS/7.0-beta/updates/RPMS/squid-2.3.STABLE4-1_StackGuard_2.i386.rpm **Linux-Mandrake:** http://www.linux-mandrake.com/en/ftp.php3	Squid /tmp File Race Condition	Medium	Bug discussed in newsgroups and websites.

[54] Immunix OS Security Advisory, IMNX-2000-70-023-01, January 10, 2001.
[55] Linux-Mandrake Security Update Advisory, MDKSA-2001:010, January 10, 2001.
[56] Immunix OS Security Advisory, IMNX-2000-70-022-01, January 10, 2001.
[57] Linux-Mandrake Security Update Advisory, MDKSA-2001:001, January 10, 2001.
[58] Immunix OS Security Advisory, IMNX-2000-70-020-01, January 10, 2001.
[59] Linux-Mandrake Security Update Advisory, MDKSA-2001:009, January 10, 2001.
[60] Immunix OS Security Advisory, IMNX-2000-70-018-01, January 10, 2001.
[61] Linux-Mandrake Security Update Advisory, MDKSA-2001:003, January 10, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Multiple Vendors[62, 63]	Unix	RedHat Linux 7.0; Wirex Immunix OS 7.0-Beta; Linux-Mandrake 6.0, 6.1, 7.0, 7.1, 7.2	A race condition vulnerability exists in the creation and handling of /tmp files that could let a malicious user overwrite or append system files.	Upgrade available at: **Wirex Immunix OS 7.0-Beta:** available: http://www.immunix.org/ImmunixOS/7.0-beta/updates/RPMS/arpwatch-2.1a10-29_StackGuard_2.i386.rpm **Linux-Mandrake:** http://www.linux-mandrake.com/en/ftp.php3	Arpwatch /tmp File Race Condition	Medium	Bug discussed in newsgroups and websites.
Multiple Vendors[64, 65, 66, 67, 68]	Unix	GnuPG 1.0-1.0.3b	A vulnerability exists when importing keys from public key servers, GnuPG will import private keys (also known as secret keys) in addition to public keys. If this happens, the user's web of trust becomes corrupted.	**RedHat:** ftp://updates.redhat.com **Trustix:** http://www.trustix.net/pub/Trustix/updates/ **Linux-Mandrake:** http://www.linux-mandrake.com/en/ftp.php3 **Debian:** http://security.debian.org/dists/stable/updates/main/ **Conectiva:** ftp://atualizacoes.conectiva.com.br	GnuPG Detached Signature Verification False-Positive	Medium	Bug discussed in newsgroups and websites.
NetScreen[69]	Multiple	Screen OS 1.73r1, 2.10r3, 2.1r6, 2.5r1	A buffer overflow vulnerability exists which could allow a malicious user to cause a Denial of Service.	NetScreen has release a fix available at: http://www.netscreen.com/support/updates.html	NetScreen Firewall Denial of Service CVE name: CAN-2001-0007	Low/ **High** **(High if DDos best-practices not in place)**	Bug discussed in newsgroups and websites. Exploit script has been published.
Oracle Corporation[70]	Unix	Internet Application Server 3.0.7 and Previous	A documented backdoor exists in the combination of Apache and WebDB software which could allow a remote malicious user unauthorized access to critical resources.	No workaround or patch available at time of publishing.	Oracle Apache+ WebDB Documented Backdoor	**High**	Bug discussed in newsgroups and websites.
Oracle Corporation[71]	Unix	Internet Application Server 3.0.7 and Previous	Configuration vulnerabilities exist in the WebDB/Portal Listener modplsql and PL/SQL procedures that could allow a remote malicious user to gain database access.	Workaround can be found at: http://otn.oracle.com/deploy/security/alerts.htm	Oracle WebDB/Portal Listener Modplsql and Public PL/SQL Procedure Database Access	Medium	Bug discussed in newsgroups and websites.

[62] Immunix OS Security Advisory, IMNX-2000-70-017-01, January 10, 2001.
[63] Linux-Mandrake Security Update Advisory, MDKSA-2001:002, January 10, 2001.
[64] Red Hat, Inc. Red Hat Security Advisory, RHSA-2000:131-02, December 19, 2000.
[65] Trustix Security Advisory, December 20, 2000.
[66] Linux-Mandrake Security Update Advisory, MDKSA-2000:087, December 20, 2000.
[67] Debian Security Advisory, DSA-010-1, December 24, 2000.
[68] Conectiva Linux Security Announcement, CLA-2000:368, December 29, 2000.
[69] NSFOCUS Security Advisory, SA2001-01, January 9, 2001.
[70] eSecurityOnline.com Free Vulnerability Alert 3269, December 27, 2000.
[71] eSecurityOnline.com Free Vulnerability Alert 3269, December 27, 2000.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
RedHat[72]	Unix	NSA Security-Enhanced Linux slinux-200012181053	A buffer overflow vulnerability exists in the libsecure/get_default_type.c file, which could allow a malicious user to modify data contained in other memory locations.	Upgrade available at: http://www.nsa.gov/selinux/updates-200101020953.tgz	Security-Enhanced Linux Buffer Overflow	Medium	Bug discussed in newsgroups and websites.
StorageSoft[73]	Windows 95/98/NT 4.0/2000, Unix	ImageCast IC3 4.1	A Denial of Service vulnerability exists when long strings to the ICCC service, listening on port 12002, are sent.	No workaround or patch available at time of publishing.	ImageCast Denial of Service	Low	Bug discussed in newsgroups and websites.
Sun Micro-systems, Inc.[74]	Unix	Solaris 2.5.1, 2.6, 7.0, 8.0	A vulnerability exists in the creation of /tmp files by patchadd, which could let a malicious user gain elevated privileges, corrupt system files, or execute arbitrary commands.	No workaround or patch available at time of publishing.	Solaris Patchadd Race Condition	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
Sun Micro-systems, Inc.[75]	Unix	Solaris 2.6, 7.0, 8.0	A Denial of Service vulnerability exists when a file is created in the /var/mail directory using the extension $LOGNAME.	Unofficial workaround (eSecurityOnline): Remove any lock files in /var/mail.	Solaris Mailx Lockfile Denial of Service	Low	Bug discussed in newsgroups and websites. Script has been published.
Sun Micro-systems, Inc.[76]	Unix	Sun Solaris 2.5.1, 2.5.1_x86, 2.6, 2.6_x86, 7.0, 7.0_x86, 8.0, 8.0_x86	A vulnerability exists in the creation of temporary files by the catman program, which could let a malicious user overwrite or corrupt files owned by other users.	No workaround or patch available at time of publishing.	Solaris Catman Race Condition	Medium	Bug discussed in newsgroups and websites. Exploit scripts have been published.
Sun Micro-systems, Inc.[77]	Unix	Solaris 2.4, 2.5, 2.5.1, 2.6	A buffer overflow vulnerability exists in the exrecover binary, which could let a malicious user overwrite stack variables and potentially arbitrarily execute code.	Current workaround is to remove the setuid bit from the exrecover program.	Solaris Exrecover Buffer Overflow	**High**	Bug discussed in newsgroups and websites.
SuSE[78]	Unix	Linux 7.0	A Denial of Service vulnerability exists in the way long file names are handled. It may be possible for a malicious user to execute arbitrary code, deny service to legitimate users, and potentially break out of a chroot environment.	No workaround or patch available at time of publishing.	Linux ReiserFS Kernel Oops and Code Execution	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
Technote Inc.[79]	Windows NT 4.0/2000	Technote Pro, 2000, 2001	A vulnerability exists in the main.cgi script, which could allow a remote malicious user to view arbitrary files, and possibly also execute arbitrary commands.	No workaround or patch available at time of publishing.	Technote 'filename' Variable File Disclosure	**High**	Bug discussed in newsgroups and websites. Exploit has been published.

[72] Bugtraq, December 26, 2000.
[73] Defcom Labs Advisory, def-2001-01, January 8, 2001.
[74] Bugtraq, December 18, 2000.
[75] eSecurityOnline Free Vulnerability Alert 3275, January 3, 2001.
[76] Vapid Labs Advisory ID, 11242000-02, December 18, 2000.
[77] Bugtraq, January 9, 2001.
[78] Bugtraq, January 10, 2001.
[79] Ksecurity Advisory, December 27, 2000.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Technote Inc.[80]	Windows NT 4.0/2000	Technote 2000, 2001, Pro	A vulnerability exists in the print.cgi script, which could let a remote malicious user execute arbitrary commands.	No workaround or patch available at time of publishing.	Technote 'board' Function File Disclosure	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
Tiny Software[81]	Windows 95/98/ME/ NT 4.0/2000	WinRoute 4.1	A vulnerability exists in the default installation, which can indirectly affect the stability and security of the machine. Malicious software such as viruses will find it easier to corrupt the system or hijack system processes, and penetrate a WinRoute system protected by a firewall.	No workaround or patch available at time of publishing.	WinRoute Pro Memory Protection Disabling	Medium/ **High** **(High if DDoS best-practices not in place)**	Bug discussed in newsgroups and websites.
Tiny Software [82]	Windows 95/98/ME/ NT 4.0/2000	WinRoute 4.1	A vulnerability exists in the User Accounts option that could let a malicious user use sniffed Windows domain usernames and passwords to access a Windows network and launch further attacks.	No workaround or patch available at time of publishing.	Tiny WinRoute Pro Authentication	Medium/ **High** **(High if DDoS best-practices not in place)**	Bug discussed in newsgroups and websites.
Upland Ltd[83]	Multiple	Upland Solutions 1st Up Mail Server 4.1	A remote Denial of Service vulnerability exists in the "mail from" field.	Upgrade to version 1st Up Mail Server 4.1.4e available at: http://www.upland.co.uk/1stup/UpMailSetUp.EXE	1st Up Mail Server Denial of Service	Low	Bug discussed in newsgroups and websites.
Voyant Technol-ogies[84]	OS/2, Unix	Sonata 3.0	Sonata comes with a program installed setuid root that will execute supplied arguments, which could let a malicious user gain root privileges.	No workaround or patch available at time of publishing.	Sonata Local Arbitrary Command Execution	**High**	Bug discussed in newsgroups and websites.
WebMaster Technol-ogies[85]	Windows 98/NT 4.0/2000, Unix	WebMaster Conference Room 1.8.1	A Denial of Service vulnerability exists when duplicate connections are made.	Upgrade available at: http://www.webmaster.com/products/	WebMaster Conference Room Developer Edition Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit has been published.

[80] Bugtraq, December 23, 2000.
[81] NTSecurity, January 2, 2001.
[82] Securiteam, January 9, 2001.
[83] USSR Labs Advisory Code, USSR-2000058, December 25, 2000.
[84] Bugtraq, December 18, 2000.
[85] Bugtraq, January 10, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Zope[86]	Unix	Zope 1.10.3, 2.1.x, 2.2.-2.2.4	A vulnerability exists in the way Zope calculates roles which could let a malicious user gain elevated privileges.	**RedHat:** ftp://updates.redhat.com/powertools **Conectiva:** ftp://atualizacoes.conectiva.com.br **Debian** http://security.debian.org/dists/frozen/updates/main/source/ **Linux-Mandrake:** http://www.linux-mandrake.com/en/ftp.php3	Zope Unauthorized Role Access CVE name: CVE-2000-0725	Medium	Bug discussed in newsgroups and websites.

*Risk is defined in the following manner:

High - A vulnerability that will allow an intruder to immediately gain privileged access (e.g., sysadmin, and root) to the system. An example of this would be a vulnerability in which a sequence of instructions is sent to a machine by an unauthorized user and the machine responds with a command prompt.

Medium - A vulnerability that will allow an intruder immediate access to the system that is not privileged access. This allows the intruder the opportunity to continue the attempt to gain root access. An example would be a configuration error that allows an intruder to capture the password file.

Low - A vulnerability that provides information to an intruder that could lead to further compromise attempts or a Denial-of-Service (DoS) attack. The reader should note that while the DoS attack is deemed low from a threat potential, the frequency of this type of attack is very high. DoS attacks against mission-critical nodes are not included in this rating and any attack of this nature should instead be considered as a "High" threat.

Recent Exploit Scripts/Techniques

The table below contains a representative sample of exploit scripts and How to Guides, identified between December 18, 2000 and January 9, 2001, listed by date of script, script names, script description, and comments. **Items listed in boldface/red (if any) are attack scripts/techniques for which vendors, security vulnerability listservs, or Computer Emergency Response Teams (CERTs) have not published workarounds or patches, or which represent scripts that malicious users are utilizing**. During this period, 39 scripts, programs, and net-news messages containing holes or exploits were identified.

Date of Script (Reverse Chronological Order)	Script name	Script Description
January 9, 2001	Sa2001_01.txt	Perl exploit script for the NetScreen Firewall / VPN Appliance overflow vulnerability.
January 8, 2001	Exhpcu.c	Script which exploits the HP-UX v11.00 /bin/cu local buffer overflow vulnerability.
January 5, 2001	Portscan.pdf	Document about known techniques used to determine open/closed ports on a host and ways a malicious user may identify the network services running on arbitrary servers.
January 4, 2001	Aasniff.Tar.gz	A kernel patch which hides a sniffer from the most known anti-sniffers.
January 4, 2001	Sara-3.3.2.Tar.gz	A security analysis tool based on the SATAN model.
January 3, 2001	**Guninski31.txt**	Exploit code for the Windows Media Player Javascript URL vulnerability.

[86] Securiteam, December 19, 2000.

Date of Script (Reverse Chronological Order)	Script name	Script Description
January 3, 2001	**Mailx-lock.sh**	Exploit script for the Solaris mailx Lockfile Denial Of Service vulnerability.
January 3, 2001	Ssh-2.4.0.tar.gz	SSH (Secure Shell) is a program to log into another computer over a network, to execute commands in a remote machine, and to move files from one machine to another.
January 1, 2001	**Wu-ftpd-solsparc.c**	Remote root exploit script, which uses the site exec format string vulnerability.
January 1, 2001	**Xgtk.C**	A local exploit for any set*id program which uses Gtk+ up to v1.2.8.
December 31, 2000	7350wu-V5.Tar.gz	Remote root exploit script that works on Linux/x86 and FreeBSD.
December 31, 2000	Ngst-0.3b.Tar.gz	An active packet sniffer, based on libpcap and libnet, which dumps into a file the payload of all the packets received on the specified ports.
December 30, 2000	Hhp-fancy_smash.c	A local root exploit script, which exploits the Fancylogin v0.99.7 vulnerability.
December 30, 2000	Hhp-gnomehack_smash.c	A local buffer overflow exploit script for Debian 2.2.
December 30, 2000	Hhp-kwintv_smash.c	A Kwintv local buffer overflow exploit script for SuSE 7.0.
December 30, 2000	Saint-3.1.3.Beta1.Tar.gz	An updated version of SATAN, designed to assess the remote security of computer networks.
December 30, 2000	Scx-sa-12.txt	Proof of concept code for the Apache 1.3.14 vulnerability.
December 27, 2000	Hhp-stonx_smash.c	Local root exploit script for the STonX v0.6.5 and v0.6.7 vulnerability.
December 26, 2000	Pdump-0.8.Tar.gz	A sniffer that dumps, greps, monitors, creates, and modifies traffic on a network.
December 26, 2000	Sendip-1.4.Tar.gz	A command line tool which sends arbitrary IP packets and has a large number of command line options to specify the content of every header of a TCP, UDP, ICMP, or raw IP packet, and allows any data to be added to the packet.
December 26, 2000	Xxconq.C	Local root exploit script for the Linux xconq v7.4.1 vulnerability.
December 25, 2000	**Sparc_ftpd.c**	Solaris 2.8 remote ftpd exploit script, which uses a site exec format string vulnerability.
December 23, 2000	**Catman-race.txt**	Proof of concept exploit for the Solaris 2.7/2.8 /usr/bin/catman vulnerability.
December 23, 2000	Gre.pdf.gz	Paper that describes a possible way to attack hosts with RFC1918 IP addresses behind GRE Tunnels over the Internet.
December 23, 2000	Icmp_scanning_v2.5.pdf	Paper that outlines what can be done with the ICMP protocol regarding scanning and includes details on plain Host Detection techniques, Advanced Host Detection techniques, Inverse Mapping, Trace routing, OS fingerprinting methods with ICMP, and which ICMP traffic should be filtered on a Filtering Device.
December 22, 2000	Saint-3.1.2.Tar.gz	An updated version of SATAN, designed to assess the remote security of computer networks.
December 21, 2000	**Ksh.temp-hole.txt**	Demonstration exploit for the Korn Shell (ksh) temp file vulnerability.
December 21, 2000	Sara-3.3.1.Tar.gz	A security analysis tool based on the SATAN model.
December 19, 2000	Cgichk_2.50.Tar.gz	A web vulnerability scanner which automatically searches for a series of interesting directories and files on a given site. Instead of focusing on vulnerable CGI scripts, it looks for interesting and/or hidden directories such as logs, testing, secret, scripts, stats, restricted, code, robots.txt, etc.
December 19, 2000	Obsd-ftpd.c	Script which exploits the OpenBSD v2.6 and 2.7 ftpd remote root vulnerability.

Date of Script (Reverse Chronological Order)	Script name	Script Description
December 18, 2000	7350nxt-V3.Tar.gz	Exploit script for the Bind NXT remote root vulnerability, which affects Bind v8.2 - 8.2.2.
December 18, 2000	7350oftpd.Tar.gz	Exploit script for the ftpd Single Byte Buffer Overflow vulnerability.
December 18, 2000	**Catman-race.pl**	Script which exploits the Solaris catman Race Condition vulnerability.
December 18, 2000	**Ctman-race2.pl**	Script which exploits the Solaris catman Race Condition vulnerability.
December 18, 2000	Fm.c	Script which exploits the Firewall-1 Fast Mode TCP Fragment vulnerability.
December 18, 2000	Mimedefang-0.7.Tar.gz	A MIME e-mail scanner that alters or deletes various parts of a MIME message according to a flexible configuration file.
December 18, 2000	Ssh-2.3.0.Tar.gz	SSH (Secure Shell) is a program to log into another computer over a network, to execute commands in a remote machine, and to move files from one machine to another.
December 18, 2000	Xckermit.C	Exploit script for the Ckermit v7.0 local buffer overflow vulnerability.
December 18, 2000	**Xitetris.C**	Script which exploit the Itetris Privileged Arbitrary Command Execution vulnerability.

Trends

Probes/Scans:

The CERT/CC has received reports of extensive probing to port 515/tcp. For more information see CERT Advisory CA-2000-22 Input Validation Problems in LPRng, located at: http://www.cert.org/advisories/CA-2000-22.html.

Other:

Several instances of remote self-updating viruses have been reported. In addition, the most recent virus incorporates strong cryptography to avoid detection.

Viruses

PE_BEGEMOT.A (Aliases: BEGEMOT.A,, PE_BEGEMOT.A-O, Win95.Begemot) (File Infector Virus): This memory-resident, polymorphic virus infects all PE files that include executable (EXE) files and screensaver (SCR) files. Besides infecting files, it adds an infected executable file inside the archive files with the extension of .RAR. On the 2nd day of January this virus displays a message box and deletes antivirus files.

PE_DEMIURG.A (Alias: DEMIURG.A) (File Infector Virus): Several reports of infection of this virus have been reported in Taiwan. It infects Windows EXE files (PE files), DOS COM files, BAT files (batch files), and .XLS files (Excel 97 worksheets). When the infected user's computer is rebooted, the virus automatically becomes memory resident via the infected KERNEL32.DLL. This virus also drops a macro virus named “DEMIURG.XLS” in the Excel Start folder, which is automatically loaded by Excel 97 when the application is started. This macro virus is detected as X97M_DEMIURG.A.

PE_KRIZ.3862 (Alias: KRIZ.3862) (File Infector Virus): This memory-resident polymorphic Windows virus infects EXE and SCR files. It has a destructive payload, which is triggered on December 25. On this date, this virus attempts to destroy certain types of PC Flash BIOS (similar to PE_CIH) and the infected computer's CMOS information.

PE_KRIZ.4271 (Aliases: KRIZ.4271, PE_KRIZ.4271-O, W32/Kriz.4070, Win32.Kriz.4271) (File Infector Virus): This memory-resident polymorphic Windows virus infects EXE and SCR files. It has a destructive payload, which is triggered on December 25. On this date, this virus attempts to destroy certain types of PC Flash BIOS (similar to PE_CIH) and the infected computer's CMOS information.

PE_RESUR (Aliases: RESUR, W32/Resur, W32.Resurdbg, Win32/Resurrection) (File Infector Virus): This PE virus infects selected Win32 programs in the Windows directory. Infected files do not execute normally and perform illegal operations. This virus does not have a destructive payload.

PE_SST.952 (Alias: SST.951) (File Infector Virus): This memory resident, non-polymorphic virus replicates itself. It modifies the Interrupt Descriptor Table (IDT) and then resides in the system memory. To infect, it appends itself at the end of the host file. It does not have a destructive payload and it does not reinfect previously infected files. The virus identifies infected files with the image version or the PE header offset of the file. If this is equal to " SST," the file is already infected. The virus program contains the following text string:

```
All only begins..
Viral Hazard Crew moves to the win32 arena !
<Win9x.SST.952>
```

PE_WIT.A (Alias: WIT.A) (File Infector Virus): This virus has been reported in the wild. It infects PE files with the EXE extension. Upon execution, the virus drops a copy of itself in the Windows System directory with the file name, “DXINIT3D.EXE” and then modifies the following registry entries so that it is executed each time an infected file is opened:

```
HKEY_CLASSES_ROOT\exefile\shell\open\command\
(Default)=“”%SysDir%\DXINIT3D.EXE&”/I&E%1%*””
HKEY_LOCAL_MACHINE\Software\CLASSES\exefile\shell\open\command\
(Default)=“”%SysDir%DXINIT3D.EXE”/I&E%1%*””
```

The virus copies itself into the target file and modifies the extension of the EXE file to WX3. Infected files contain the following text string:

```
[X3] by Wit AKA CyberViper.2000.
```

PIF_IBLIS.A (Alias: IBLIS.A) (IRC Script Worm): This worm propagates via Internet Relay Chat (IRC). It arrives as a fake text file containing a password for a pornographic Web site.

VBS/MBot-A (Visual Basic Script Worm): This is a VBS e-mail worm, which works in a similar way to VBS/Loveletter. The worm arrives as an e-mail attachment and is called "matrixbot.vbs." The e-mail will have the subject line "NewsMatrixBot [Test Run only]" and the body text "NewsMatrix Bot [Test Run only] if you send me anymore advertisement and there's gonna other bot coming. You can get the cure at http://www.ashoppe.net -People2People Chat (ask the AI for the cure)." If the worm is run, it will copy itself to the Windows directory as "Win32DLL.vbs" and to the Windows System directory as "MSKernel32.vbs" and as "matrixbot.vbs." It will also change the registry so that the first two files are run automatically. It also sets the IE start page to "http://www.ashoppe.net." The worm then uses Outlook to send itself to all addresses in the address book.

VBS/Mcon-B (Visual Basic Script Worm): This worm spreads via network shares and mIRC. The worm copies itself to the Windows Fonts directory and installs itself in the registry so that it is run at startup. The worm will go into an infinite loop by pinging random addresses.

VBS_SEASON.A (Alias: SEASON.A) (Visual Basic Script Worm): This destructive VBScript virus spreads via Internet Relay Chat (IRC) channels and diskette drives. Upon execution and after infection, it displays message boxes. This virus, when executed for a second time, deletes files with certain extensions in the "My Documents" folder.

VBS/Sheep-A (Visual Basic Script Worm): This virus is a mIRC (Internet Relay Chat) worm that arrives as a file called: CounterstrikeRP.TXT.vbs. The worm adds a hundred spaces before the .VBS extension in an attempt to hide the fact that the attachment is a Visual Basic Script file. The worm alters mIRC to send itself automatically. When executed the file copies itself to "C:\WINDOWS\system\RP.TXT.vbs" and "C:\WINDOWS\Start Menu\Programs\StartUp\Startup§.vbs." On the 1st, 5th, 10th, 15th, 20th or 25th of the month, it will attempt to use the file CounterStrikeRP.BMP as tiled wallpaper.

VBS/Tqll-A (Visual Basic Script Worm): This worm arrives as an e-mail attachment called 'happynewyear.txt.vbs' which has the subject line 'New Year !' and the body text 'Wow Happy New Year !'. The worm will attempt to use Outlook to mail itself to everyone in the address books. The worm also drops a copy of Troj/Downloader (see Trojan Section).

W32/Hybris-D (Win32 Worm): This worm has been reported in the wild. It is a worm capable of updating its functionality over the Internet. It consists of a base part and a collection of upgradeable components. The components are stored within the worm body encrypted with 128-bit strong cryptography. When run, the worm infects WSOCK32.DLL. Whenever an e-mail is sent, the worm attempts to send a copy of itself as an attachment to a separate message to the same recipient. Any other behavior exhibited by the worm is entirely dependent on the set of installed components. The text of the e-mail message is determined by one of the installed components, and can be changed by an upgrading mechanism. The message can have any subject, any message text and any filename for the attached file. A common component of the worm checks the language settings of the computer it has infected, and selects a message from English, French, Portuguese, and Spanish. The methods for upgrading the worm can also be changed since they are upgradeable components. One of the upgrading techniques attempts to download the encrypted components from a website that is presumably operated by the worm author. This website has since been disabled. However, this component could be upgraded to have a different web address. The other method involves posting its current plug-ins to the Usenet newsgroup alt.comp.virus, and upgrading them from other posts by other infections of the worm. These are in encrypted form, and have a header with a four character identifier and a four character version number, in order for the worm to know which plug-ins to install. Another component of the worm searches the PC for .ZIP and .RAR archive files. When it finds one, it searches inside it for a .EXE file, which is renamed to .EX$, and then adds a copy of itself to the archive using the original filename.

There is a payload component, which on the 24th of September of any year, or at 1 minute to the hour at any day in the year 2001, displays a large animated spiral in the middle of the screen. There is also a component that applies a simple polymorphic encryption to the worm before it gets sent by e-mail. By upgrading this component the author is able to completely change the appearance of the worm in unpredictable ways in an attempt to defeat anti-virus products detecting it.

W32/Navidad-B (Windows 32 Executable FileVirus): This virus has been reported in the wild. It arrives in an e-mail message with an attachment called EMANUEL.EXE. If the attached program is launched, it displays a dialog box containing the text ;")." The worm then attempts to read new e-mail messages and to send itself to the senders' addresses. The worm copies itself into the Windows system directory with the filename WINTASK.EXE and changes the registry so that it runs on Windows startup and before any file is run. The worm also installs itself into the system tray. If the user clicks on the icon, it displays a dialog box with the text "Nunca presionar este boton." If the user clicks the button, the worm displays a dialog box with the title "Emmanuel....." and the text "Emmanuel-God is with us! May god bless u. And Ash, Lk and LJ!!." If the user does not press the button but instead attempt to close the message the worm displays a message with the title "Emmanuel....." and the text "May GOd bless u;D."

W97M_MARKER.FQ (Aliases: MARKER.FQ, MARKER.Q) (Word 97 Macro Virus): This Word 97 macro virus infects upon closing an active document. It modifies document properties, but it has no destructive payload. It utilizes Word’s built in Random Number Generator to execute its payload. If the random number generated is less than 0.3, the virus sets the properties of the infected document as follows:

TITLE: ETHAN FROME
AUTHOR: EW/LN/CB
KEYWORDS: ETHAN

W97M_METYS.K (Alias: METYS.K) (Word 97 Macro Virus): This non-polymorphic, non-destructive macro virus infects active Word documents. On its trigger date, September 18, messages are displayed. The virus generates some random numbers and depending upon those numbers further messages are displayed.

W97M_MYNA.AA (Aliases: MYNA, W97M/MYNA.Gen, W97M.MYNA.Variant, Macro.Word97.Myna.z, W97M.MYNA) (Word 97 Macro Virus): This is a variant of the W97M_MYNA family of macro viruses. The original version of this virus has three macros: “Document_Close," “Document_Open," and “Document_New." In this variant, the code of the second macro is interspersed with the first one. The “Document_Open” or “Document_New” events activate the macro virus. The virus then attempts to infect all currently open documents. It checks all modules of the target documents and infects only those with the “ThisDocument” module. It does not infect documents with the following string: MYNAMEISVIRUS. Like the original W97M_MYNA, this disables the macro VirusProtection option, but it corrupts “Document_Close” wherein closing a document prompts an error message.

WM97/Chronic-A (Word 97 Macro Virus): WM97/Chronic-A has a complex trigger mechanism and under some circumstances can overwrite the CMOS. The virus maintains a count of the number of times the viral code is executed. Every 25th time the code runs (25, 50, 75, etc) the virus runs the payload. The payload consists of a complex series of checks on the day part of the date. If the day part of the date can be divided exactly by 5, the virus will attempt to set the write password for the current document to a value gained from the system. The password will normally be "1297307460." The main part of the payload consists of modifying the first 1020 bytes of specific files and also appending the text "Karachi_y2k7" to those same files. The specified file paths are generally only found under the Windows 95 and Windows 98 operating systems. Every time the payload runs the following files are affected:

"C:\WINDOWS\SOL.EXE"
"C:\WINDOWS\MSHEARTS.EXE"
"C:\WINDOWS\FREECELL.EXE."

Various files are affected depending on whether the day can be divided exactly by 3, divided exactly by 3 and by 6, and divided exactly by 3 and by 6 and by 9. If the day can be divided exactly by 2, the virus will attempt to print between 1 and 9 copies of the current document. If the day can also be divided exactly by 4, the virus will modify "C:\WINDOWS\WIN.COM" to contain the Trojan Troj/KillCMOS-E (see Trojan Section) which is a Trojan that overwrites the CMOS settings with random data. This will be run the next time that Windows is restarted. If the day can also be divided exactly by 6, the virus will copy "C:\WINDOWS\WIN.COM" to "WIN.ORG" and then create a new "C:\WINDOWS\WIN.COM" with the Trojan Troj/KillCMOS-E which will be run the next time Windows is restarted.

WM97/Eight941-R (Word 97 Macro Virus): This is a macro virus, which spreads but does not have a working payload.

WM97/Ethan-DT (Word 97 Macro Virus): This is a variant of the WM97/Ethan Word macro virus, which has been created due to interactions between the original WM97/Ethan virus and user macros.

WM97/Footer-V (Word 97 Macro Virus): WM97/Footer-V is a Word macro virus. The virus has been created by merging the WM97/Class-D and WM97/Footer-A Word macro viruses.

WM97/Hope-AA (Word 97 Macro Virus): This virus is an amalgamation of WM97/Hope-S, WM97/Class-D and WM97/Story. Only the WM97/Hope-S part of the virus runs and this section has no payload. The payloads that are normally associated with WM97/Class-D and WM97/Story will not run as the virus produces errors as it tries to replicate.

WM97/Marker-CK (Word 97 Macro Virus): WM97/Marker-CK is a variant of the WM97/Marker Word macro virus. Whenever an infected document is closed there is a 1 in 3 chance of a File Summary box appearing on the screen with the author name set to Ethan Frome.

WM97/Marker-GB (Word 97 Macro Virus): This variant of the Marker family keeps a log file of infections. It may save this log file to C:\hsf*.sys, where * is a number. It will also create and run the file C:\netldx.vxd, which contains instructions to send the log file via FTP.

WM97/Media-A (Word 97 Macro Virus): WM97/Media-A is a Word macro virus. The virus may display a dialog box containing the text "Dat mediatheekmens SUCKS!!!" when infecting documents.

WM97/Thus-CD (Word 97 Macro Virus): WM97/Thus-CD is a variant of the WM97/Thus Word macro virus. However, this variant of the virus has no payload and does little except replicate.

Trojans

Trojans have become increasingly popular as a means of obtaining unauthorized access to computer systems. This table starts with Trojans discussed in CyberNotes #2001-01 and will be added on a cumulative basis. Trojans that are covered in the current issue of CyberNotes are listed in boldface/red. Following this table are write-ups of new Trojans and updated versions discovered in the last two weeks. Readers should contact their anti-virus vendors to obtain specific information on Trojans and their variants that their software detects. NOTE: At times, Trojans may contain names or content that may be considered offensive.

Trojan	Version	CyberNotes Issue #
BAT_EXITWIN.A		**Current Issue**
TROJ_AOL_EPEX		**Current Issue**
TROJ_AOLWAR.B		**Current Issue**
TROJ_AOLWAR.C		**Current Issue**
TROJ_AZPR		**Current Issue**
TROJ_BAT2EXEC		**Current Issue**
TROJ_BKDOOR.GQ		**Current Issue**
TROJ_GLACE.A		**Current Issue**
Troj/KillCMOS-E		**Current Issue**
TROJ_NAVIDAD.E		**Current Issue**
TROJ_QZAP.1026		**Current Issue**
TROJ_SUB7.401315		**Current Issue**
TROJ_SUB7.MUIE		**Current Issue**
TROJ_SUB7DRPR.B		**Current Issue**

BAT_EXITWIN.A: Upon execution, this Trojan's self-extracting EXE file drops the files AUTOEXEC.BAT and INSTALL.BAT in the Windows temporary directory. Thereafter, INSTALL.BAT checks for the presence of AUTOEXEC.BAT in the directory of the user's C:\ drive. If it does not find the file, it creates one and copies its own AUTOEXEC.BAT in it. If it finds the file, it appends .BAK to the extension and inserts its virus code into the host. It then displays the following message and resets the computer: You've been fucked by Th3 H@cker. Upon next startup, the infected AUTOEXEC.BAT checks for INSTALL.BAT in the Windows temporary directory. It continuously resets the computer after displaying the following message: Have fun yet??

TROJ_AOL_EPEX (Aliases: TROJ.AOL.EPEX, AOL.EPEX, AOL_EPEX, EPEX, AOL): Upon activation, this America Online (AOL), password-stealing Trojan drops a copy of itself in a hidden file found in the directory of the user's drive C:\. It then modifies registry entries to run this file at start up. This Trojan has no destructive payload.

TROJ_AOLWAR.B (Aliases: AOL War, AOLWAR.B, Trojan.Win16.AOLwar.b): This destructive Trojan, written in Visual Basic, displays images and deletes files. The Trojan executes only when the host computer is installed with VBRUN300.DLL Runtime Library. This file runs only in AOL version 5.0.

TROJ_AOLWAR.C (Aliases: AOL War, AOLWAR.C, Trojan.Win16.AOLwar.c): This destructive Visual Basic Trojan appears as an America Online (AOL) War AddOn. The Trojan executes if the host computer is installed with VBRUN300.DLL Runtime Library. It carries a payload that displays messages and deletes files.

TROJ_AZPR (Aliases: BackDoor-G2.svr.gen, AZPR): This destructive backdoor Trojan is attached to the "Advanced Zip Password Recovery Tool." This server-side hacking tool enables a remote hacker access to an infected computer and it makes itself active in memory upon execution. It is similar to the Back Orifice Trojan.

TROJ_BAT2EXEC (Alias: BAT2EXEC): This destructive Trojan formats the Hard disk automatically with a system startup file. Upon execution, the Trojan displays the text: PLEASE WAIT WHILE PROGRAM LOADS…. Then it overwrites the AUTOEXEC.BAT file with itscodes which automatically formats all drives available in the user's system. It also attempts to delete files in all drives using the command "deltree."

TROJ_BKDOOR.GQ (Aliases: BackDoor-GQ.svr, BKDOOR, BKDOOR.GQ): This Trojan is the server side of a hacking tool. It allows a remote user, running the client side of this program, access to the infected computer via the Internet. This is similar to the Back Orifice Trojan. Upon execution, it drops a copy of itself as "MSSCMC32.EXE" in the Windows directory. To enable the Trojan to run upon boot up, it adds,"MSSCMC32" to the following registry entry: HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run. Upon boot up of the host computer, the Trojan becomes active in memory and waits for commands from the client side of this hacking tool.

Troj/Downloader (Aliases: Serbian.Trojan, W95/Loader Trojan): This Trojan horse has been distributed on some sex-related Usenet newsgroups as Quickflick.mpg.exe. The filename may fool some people into believing it is a legitimate .MPG movie file. When the Trojan horse is run it attempts to download and silently run another program from a website. The program it attempts to download is believed to be a copy of Troj/Subseven a backdoor Trojan horse, but at the present time it is no longer available on the website.

TROJ_GLACE.A (Alias: GLACE.A): This backdoor Trojan program allows remote access to PCs. This Trojan program is composed of a server program and a client program. The server program drops a copy of itself as KERNEL32.EXE and SYSEXPLR.EXE in the system directory and then registers the first as a system service to ensure that it is loaded at every start-up.

Troj/KillCMOS-E is a Trojan that overwrites the CMOS settings with random data. This Trojan is dropped by M97/Chronic-A

TROJ_NAVIDAD.E (Aliases: NAVIDAD.E, NAVIDAD.B, EMMANUEL, TROJ_EMMANUEL): This malicious Internet worm uses Microsoft Messaging Application Program Interface (MAPI132.DLL) to propagate via e-mail. It replies to all messages in the e-mail INBOX and attaches a copy of itself to each reply. It also modifies the registry so that it executes at every Windows start up. This variant of the infamous TROJ_NAVIDAD.A displays error messages and prevents the infected user from running executable programs as its payload. The differences between this variant and the original Trojan are in the icon it uses, the messages it uses, and the file it drops.

TROJ_QZAP.1026 (Aliases: Qzap163, QZAP, QZAP.1026): This destructive DOS Trojan is packed using PKLITE tool. Upon execution, it deletes critical portions of the hard disk so that it can no longer be accessed upon reboot.

TROJ_SUB7.401315 (Aliases: Backdoor-G2.svr.gen, SUB7.401315): This is the server side of a backdoor hacking tool. A variant of the Subseven series of hacker tools, this Trojan installs itself and modified system files so that it is run at every Windows start up. Upon execution, the Trojan drops a copy of itself, WINREG.EXE, in the Windows directory. To run at Windows start up, it modifies the following: lineShell=EXPLORER.EXE WINREG.EXE in the SYSTEM.INI file and linerun=EXPLORER.EXE WINREG.EXE in the WIN.INI file. It then creates the following registry key containing encrypted information about the Trojan and the host file: HKEY_LOCAL_MACHINE\HARDWARE\DATA. This Trojan registers itself as a service process, which enables it to work in the background, invisible in the task list. Unlike other SubSeven versions, this Trojan notifies the hacker via ICQ of successful infection and then listens to port 1032 for the client side.

TROJ_SUB7.MUIE (Alias: SUB7.MUIE): This Trojan has been reported in the wild. The Trojan program allows remote users access to a host computer and get system information. It has two parts: the client program and the server program. The server side enables users running the client program access to the host computer via a connection to the default port, 27374.

TROJ_SUB7DRPR.B (Aliases: Multidropper.z, SUB7DRPR.B, Trojan.Win32, TrojanRunner.RSP.a): This Trojan is a dropper program for TROJ_SUB7.401315 which arrives as a REAL MEDIA (.RM) file, that appears to contain a web cam clip. It attempts to play this via Real Player while it drops the Trojan in the infected system. Upon execution, this Trojan drops, VIDEO.RM in the Windows directory. The Trojan also drops MELT.EXE, which contains the Trojan program. This file moves its contents to WINREG.EXE in the Windows directory and then deletes MELT.EXE. WINREG.EXE then works in the background as a server allowing a remote user running the client side of the program to access the infected computer.